**Amendments to the Claims**

1. (canceled)

2. (currently amended) A method of providing an award on a network of gaming machines comprising:

encrypting a message on the network at a server;

transmitting the message to one of the gaming machines;

decrypting the message at the gaming machine; and

paying an award responsive to the message.

3. (previously presented) The method of claim 2 wherein the encrypting the message and decrypting the message is accomplished with a private key pair.

4. (previously presented) The method of claim 2 wherein encrypting the message comprises signing the message.

5. (previously presented) The method of claim 2 wherein encrypting the message comprises verifying the message.

6. (previously presented) The method of claim 2 wherein encrypting the message comprises both signing and verifying the message.

7. (previously presented) The method of claim 3 wherein said method further comprises periodically changing the private key pair.

8. (previously presented) The method of claim 7 wherein said method further comprises identifying the key pair that encrypted the message.

9. (previously presented) The method of claim 8 wherein identifying the key pair comprises associating a session number with each key pair.

10. (currently amended) A method for encrypting communications on a network of gaming machines comprising:

establishing a first key at a first node associated with a gaming machine;

establishing a second key at a second node on the network remote from the gaming machine;

encrypting an award payment message at ~~one of the nodes~~ at the second node;

transmitting the message to the ~~other~~ first node; and

decrypting the message at the second node and operating upon the message at the second node.

11. (previously presented) The method of claim 10 wherein the message originates at the first node and includes data indicating an amount played at the gaming machine.

12. (previously presented) The method of claim 11 wherein said second node is associated with a network computer that receives messages from multiple gaming machines on the network, said messages each including data indicating an amount played on one of the gaming machines.

13. (previously presented) The method of claim 10 wherein the encrypting the message and decrypting the message is accomplished with a private key pair.

14. (previously presented) The method of claim 10 wherein encrypting the message comprises signing the message.

15. (previously presented) The method of claim 10 wherein encrypting the message comprises verifying the message.

16. (previously presented) The method of claim 10 wherein encrypting the message comprises both signing and verifying the message.

17. (previously presented) The method of claim 13 wherein said method further comprises periodically changing the private key pair.

18. (previously presented) The method of claim 17 wherein said method further comprises identifying the key pair that encrypted the message.

19. (previously presented) The method of claim 18 wherein identifying the key pair comprises associating a session number with each key pair.

20. (previously presented) The method of claim 10 wherein the message originates at the second node and includes data indicating a bonus payable at the gaming machine.

21. (currently amended) A network of gaming machines comprising:

a first node associated with a gaming machine on the network;

a second node located on the network remote from the first node to transmit award payment messages;

a key pair, one key being associated with the first node and the other key being associated with the second node; ~~and~~

a process operable at each node to encrypt messages between the nodes using the key pair; and

a process operable at the first node to decrypt the payment award messages from the second node.

22. (previously presented) The network of claim 21 wherein said key pair comprises a private key pair.

23. (previously presented) The network of claim 22 wherein said key pairs are periodically changed and wherein said network further comprises a process operable to identify each key pair.